

CLAIMS

1 1. A method for enabling strong mutual authentication on a computer network comprising the
2 steps of:
3 transmitting a first indicia to a first computer over a first communication channel;
4 generating by said first computer a first authentication number, a second authentication
5 number, and a third authentication number;
6 transmitting by said first computer a first message to a second computer, wherein said
7 first message comprises said first authentication number encrypted by said second
8 authentication number;
9 transmitting by said first computer a second message to a verifier over a second
10 communication channel, wherein said second message comprises said second
11 authentication number encrypted and said third authentication number;
12 decrypting by said verifier said second message to obtain a first decrypted message,
13 wherein said first decrypted message comprises said second authentication
14 number;
15 transmitting by said verifier said second authentication number to said second computer

16 over a third communication channel;

17 decrypting by said second computer said first message transmitted by said first computer

18 to recover said first authentication number;

19 transmitting by said second computer a third message to said first computer over said first

20 communication channel, wherein said third message comprises said second

21 authentication number encrypted by said first authentication number; and

22 validating said second computer by said first computer by decrypting said third message

23 to obtain said second authentication number.

1 2. The method of claim 1, wherein said first authentication number is a session number.

1 3. The method of claim 1, wherein said first indicia is login information of a user for the said

2 first computer.

1 4. The method of claim 1, wherein said second authentication number is a random number.

1 5. The method of claim 1, wherein said third authentication number is a random number.

1 6. The method of claim 1, wherein said first message further comprises said first authentication

2 number encrypted with said second authentication number.

1 7. The method of claim 1, wherein said second message further comprises an encrypted portion.

1 8. The method of claim 7, wherein said encrypted portion further comprises said second
2 authentication number encrypted in response to said first indicia.

1 9. The method of claim 8, wherein said encrypted portion further comprises said first indicia
2 encrypted with a private key.

*al
CON* 10. The method of claim 1, wherein said first decrypted message is decrypted by said verifier to
2 validate said first computer to said verifier by recovering said third authentication number
3 from said first decrypted message.

1 11. The method of claim 1, wherein said third message further comprises a third indicia.

1 12. The method of claim 11, wherein said third indicia and said second authentication number
2 are encrypted with said first authentication number.

1 13. The method of claim 1, wherein said first communication channel is a confidential
2 communication channel.

1 14. The method of claim 7, wherein said verifier has tamperproof memory and processing to
2 ensure the validity of said second message or said encrypted portion of said second message.

1 15. The method of claim 1, wherein said third communication channel is an output device.

1 16. The method of claim 1, wherein transmitting said second message further comprises the steps
2 of starting a clock by said first computer and measuring a timeout period by said clock

3 wherein said timeout period defines the period of time during which said third message must
4 be received by said first computer.

1 17. The method for authenticating a third device to a first device comprising the steps of:
2 encrypting a first key with a second key by said first device encrypting said second key
3 with a third key by said first device;
4
5 decrypting said encrypted second key in response to said third key by a second device;
6 and
7 decrypting by said third device said encrypted first key using said second key obtained
8 from said second device.

1 18. The method of claim 17 further comprising the step of encrypting said second key with said
2 first key by said third device.

1 19. The method of claim 18 further comprising the step of decrypting said encrypted second key
2 using said first key by said first device.

1 20. The method of claim 19 further comprising the step of comparing said second key decrypted
2 using said first key with said second key used to encrypt said first key by said first device.

1 21. The method for authenticating a third device to a first device comprising the steps of:
2 transmitting by said first device a first message to said third device;

3 transmitting by said first device a second message to a second device;
4 transmitting by said second device a second key of said second message to said third
5 device; and
6 obtaining by said third device a first key of said first message using said second key of
7 said second encrypted key.

*a/11
00/17*

- 1 22. The method of claim 21, wherein said first message comprises said first key encrypted by
2 said second key.
- 1 23. The method of claim 21, wherein said second message further comprises an encrypted
2 portion.
- 1 24. The method of claim 23, wherein said encrypted portion further comprises said second key
2 encrypted by a public key.
- 1 25. The method of claim 21 further comprising transmitting by said third device a third message
2 to said first device.
- 1 26. The method of claim 25, wherein said third message comprises said second key encrypted by
2 said first key.
- 1 27. The method of claim 25 further comprising obtaining by said first device said second key of
2 said third message using said first key of said first message.

1 28. The method of claim 27 further comprising said first device comparing said second key of
2 said third message with said second key of said first message.

1 29. The method of claim 21, wherein transmitting said second message further comprises the
2 steps of starting a clock by said first device and measuring a timeout period by said clock
3 wherein said timeout period defines the period of time during which said third message must
4 be received by said first device.

1 30. A system for enabling strong mutual authenticating comprising:
2 a first transmitter;
3 a first receiver in communication with said first transmitter;
4 an output device in communication with said first receiver;
5 a second receiver in communication with said output device;
6 a second transmitter; and
7 a comparator in communication with said second transmitter and said first transmitter,
8 wherein said first transmitter transmits a first message to said second receiver over a first
9 communication channel;
10 wherein said first transmitter transmits a second message to said first receiver over a second
11 communication channel;

12 wherein said output device transmits a second key derived from said second message to said
13 second receiver over a third communication channel;

14 wherein said second transmitter transmits a third message to said comparator over said first
15 communication channel;

16 wherein said comparator compares said second key of said third message with said second
key of said first message;

*a
cont*

- 1 31. The system of claim 30, wherein said first receiver further comprises a smart card.
- 1 32. The system of claim 31, wherein said smart card comprises a tamperproof storage.
- 1 33. The system of claim 32, wherein said smart card further comprises the identification of the
2 positive identity of a user.
- 1 34. The system of claim 30, wherein said first transmitter encrypts a first key with said second
2 key to produce said first message.
- 1 35. The system of claim 30, wherein said first transmitter constructs an encrypted portion to
2 produce said second message.
- 1 36. The system of claim 35, wherein said first transmitter encrypts said second key to produce
2 said encrypted portion.

1 37. The system of claim 30, wherein said first receiver obtains said second key by decrypting
2 said second message with a public key.

1 38. The system of claim 37, wherein said first receiver retrieves said public key from its
2 computer memory.

a
cont 39. The system of claim 30, wherein said second receiver decrypts said first message with said
2 second key received from said output device to obtain said first key.

1 40. The system of claim 39, wherein said second receiver encrypts said second key received
2 from said output device with said first key of said first message to produce said third
3 message.

1 41. The system of claim 30, wherein said comparator decrypts said third message to obtain said
2 second key.

1 42. The system of claim 30, wherein said first communication channel is a confidential channel.

1 43. The system of claim 30, wherein said second communication channel is a confidential
2 channel.

1 44. The system of claim 30, wherein said third communication channel is a confidential channel.

1 45. The system of claim 30, wherein said second communication channel is a cellular
2 communication channel.

1 46. The system of claim 30 further comprises a first input device in communication with said
2 second receiver and said output device.

1 47. The system of claim 46, wherein said output device is in communication with said first input
2 device over a confidential communication channel.

1 48. The system of claim 30, wherein said first transmitter comprises a clock used to measure the
2 time period between transmitting said second message to said first receiver and receiving
3 said third message from said second transmitter.